UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/023,043	12/17/2001	David E. McDysan	RIC01059	5663

25537 7590 10/04/2010

VERIZON
PATENT MANAGEMENT GROUP
1320 North Court House Road
9th Floor
ARLINGTON, VA 22201-2909

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2435	

NOTIFICATION DATE	DELIVERY MODE
10/04/2010	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patents@verizon.com

Office Action Summary	Application No.	Applicant(s)	
	10/023,043	MCDYSAN, DAVID E.	
	Examiner	Art Unit	
	Thomas Gyorfi	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 September 2010*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *4/14/08 and 7/9/08*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-24 remain for examination. The amendment filed 9/22/10 amended claims 1, 9, 16, 21, and 22.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114 was filed in this application after a decision by the Board of Patent Appeals and Interferences, but before the filing of a Notice of Appeal to the Court of Appeals for the Federal Circuit or the commencement of a civil action. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 9/22/10 has been entered.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 4/14/08 and 7/9/08 have been considered by the Examiner.

Response to Arguments

4. Applicant's arguments with respect to claims 1-24 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

5. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

6. Claims 1, 3-9, 11-16, and 18-23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Seid (U.S. Patent 5,768,271) in view of Larson et al. (U.S. Patent 7,188,180 [originally submitted by the Applicant in the IDS of 4/14/08]).

Regarding claim 1:

Seid discloses a network system providing a virtual private network (VPN), said network system comprising: one or more egress routers having connections to an access network including an access link (Figs. 1-3), wherein said one or more egress routers transmit intra-VPN traffic to a destination host belonging to the VPN from sources within the VPN within a first access network connection (e.g. elements 742-509 of Fig. 7) and all extra-VPN traffic to the destination host from sources outside the VPN within a second access network logical connections for extra-VPN traffic, separate from the first access network connection (Figure 7, particularly elements 25-39; and col. 4, lines 1-10); and a plurality of ingress routers coupled to the one or more egress routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic, such that the intra-VPN traffic and the extra-VPN traffic are logically separated into different paths (Figure 7; and col. 8, line 20 – col. 9, line 25), whereby denial of service attacks on said access link originating from sources outside the VPN are prevented (col. 2, line 56 – col. 3, line 15).

Although Seid teaches in considerable detail how each VPN's logical connection should be guaranteed at least a minimum bandwidth regardless of the amount of traffic a node processes from sources other than said each VPN, Seid is silent regarding an explicit

recitation of prioritizing VPN traffic over non-VPN traffic. However, this limitation would have been immediately obvious to one of ordinary skill in the art by the time of the invention, as evidenced by Larson teaching the same in a related invention (col. 43, lines 5-40). The claim is thus obvious not only because the ability to prioritize VPN traffic over non-VPN traffic for quality-of-service purposes was well within the normal abilities of one of ordinary skill of the art, but moreover the technique of prioritizing VPN traffic over non-VPN traffic actively prevents denial of service attacks on the VPN (Larson: col. 42, lines 40-60; col. 44, lines 1-15).

Regarding claim 9:

Seid discloses a network system, comprising: an access network having an access link to a destination host belonging to a virtual private network (VPN), wherein said access network supports a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN (Figure 7, and col. 4, lines 1-10); one or more egress routers having connections to the access network, wherein said one or more egress routers transmit intra-VPN traffic to the destination host via the first logical connection and transmit all extra-VPN traffic to the destination host via the second logical connection (Fig. 3; col. 8, lines 13-57); a plurality of ingress routers coupled to the one or more egress routers for communication utilizing a network-based VPN protocol that logically partitions intra-VPN and extra-VPN traffic (Ibid, and also col. 7, line 62 – col. 8, line 13), such that the intra-VPN traffic and the extra-VPN traffic are logically separated into different paths (Figure 7; and col. 8, line 20 – col. 9, line 25), whereby denial of

service attacks on said access link originating from sources outside the VPN are prevented (col. 3, lines 10-15).

Although Seid teaches in considerable detail how each VPN's logical connection should be guaranteed at least a minimum bandwidth regardless of the amount of traffic a node processes from sources other than said each VPN, Seid is silent regarding an explicit recitation of prioritizing VPN traffic over non-VPN traffic. However, this limitation would have been immediately obvious to one of ordinary skill in the art by the time of the invention, as evidenced by Larson teaching the same in a related invention (col. 43, lines 5-40). The claim is thus obvious not only because the ability to prioritize VPN traffic over non-VPN traffic for quality-of-service purposes was well within the normal abilities of one of ordinary skill of the art, but moreover the technique of prioritizing VPN traffic over non-VPN traffic actively prevents denial of service attacks on the VPN (Larson: col. 42, lines 40-60; col. 44, lines 1-15).

Regarding claim 16:

Seid discloses a method of providing a virtual private network (VPN), said method comprising: in an access network including the access link, providing a first logical connection for intra-VPN traffic from sources within the VPN and a second logical connection for extra-VPN traffic from sources outside the VPN (Figure 7, and col. 4, lines 1-10); communicating, from a plurality of ingress routers to one or more egress routers, intra-VPN and extra-VPN traffic destined for a destination host, wherein said intra-VPN traffic and said extra-VPN traffic are transmitted utilizing a network-based VPN protocol that logically

partitions intra-VPN and extra-VPN traffic (col. 7, line 62 – col. 8, line 15); transmitting intra-VPN traffic from said one or more egress routers to the destination host belonging to the VPN via the first logical connection, and transmitting all extra-VPN traffic from said one or more egress boundary routers to the destination host via the second logical connection (col. 2, line 56 – col. 3, line 15), such that the intra-VPN traffic and the extra-VPN traffic are logically separated into different paths (Figure 7; and col. 8, line 20 – col. 9, line 25), whereby denial of service attacks on said access link originating from sources outside the VPN are prevented (col. 3, lines 10-15).

Although Seid teaches in considerable detail how each VPN's logical connection should be guaranteed at least a minimum bandwidth regardless of the amount of traffic a node processes from sources other than said each VPN, Seid is silent regarding an explicit recitation of prioritizing VPN traffic over non-VPN traffic. However, this limitation would have been immediately obvious to one of ordinary skill in the art by the time of the invention, as evidenced by Larson teaching the same in a related invention (col. 43, lines 5-40). The claim is thus obvious not only because the ability to prioritize VPN traffic over non-VPN traffic for quality-of-service purposes was well within the normal abilities of one of ordinary skill of the art, but moreover the technique of prioritizing VPN traffic over non-VPN traffic actively prevents denial of service attacks on the VPN (Larson: col. 42, lines 40-60; col. 44, lines 1-15).

Regarding claim 21:

Seid discloses a method for providing a virtual private network (VPN), the method comprising the steps of: intra-VPN traffic flowing from sources included in the VPN (Figure 7,

and col. 4, lines 1-10); extra-VPN traffic flowing from sources outside the VPN (Ibid); assigning a first priority level to traffic intra-VPN traffic flowing from sources included in the VPN; assigning a second priority level to traffic extra-VPN traffic flowing from sources outside the VPN; and granting, to traffic having the first priority level at the access link, precedence of access to a destination host belonging to the VPN over traffic having the second priority level (col. 10, lines 40-65; col. 12, lines 20-30), transmitting intra-VPN traffic from said one or more egress routers to the destination host via the first logical connection, and transmitting all extra-VPN traffic from said one or more egress routers toward the destination host via the second logical connection (col. 2, line 56 – col. 3, line 15), such that the intra-VPN traffic and the extra-VPN traffic are logically separated into different paths (Figure 7; and col. 8, line 20 – col. 9, line 25).

Although Seid teaches in considerable detail how each VPN's logical connection should be guaranteed at least a minimum bandwidth regardless of the amount of traffic a node processes from sources other than said each VPN, Seid is silent regarding an explicit recitation of prioritizing VPN traffic over non-VPN traffic. However, this limitation would have been immediately obvious to one of ordinary skill in the art by the time of the invention, as evidenced by Larson teaching the same in a related invention (col. 43, lines 5-40). The claim is thus obvious not only because the ability to prioritize VPN traffic over non-VPN traffic for quality-of-service purposes was well within the normal abilities of one of ordinary skill of the art, but moreover the technique of prioritizing VPN traffic over non-VPN traffic actively prevents denial of service attacks on the VPN (Larson: col. 42, lines 40-60; col. 44, lines 1-15).

Regarding claim 22:

Seid discloses a method of communicating, comprising: receiving a packet that is destined for a host within a virtual private network (col. 9, lines 4-26); determining whether the packet is originated within the virtual private network or external to the virtual private network (col. 8, lines 21-23); and forwarding the packet to the host over a first logical path or a second logical path based on the determination, wherein the first logical path is designated for traffic originating within the virtual private network and the second logical path is designated for traffic originating externally to the virtual private network (col. 2, line 49 – col. 3, line 14; col. 8, lines 5-10).

Although Seid teaches in considerable detail how each VPN's logical connection should be guaranteed at least a minimum bandwidth regardless of the amount of traffic a node processes from sources other than said each VPN, Seid is silent regarding an explicit recitation of prioritizing VPN traffic over non-VPN traffic. However, this limitation would have been immediately obvious to one of ordinary skill in the art by the time of the invention, as evidenced by Larson teaching the same in a related invention (col. 43, lines 5-40). The claim is thus obvious not only because the ability to prioritize VPN traffic over non-VPN traffic for quality-of-service purposes was well within the normal abilities of one of ordinary skill of the art, but moreover the technique of prioritizing VPN traffic over non-VPN traffic actively prevents denial of service attacks on the VPN (Larson: col. 42, lines 40-60; col. 44, lines 1-15).

Regarding claims 3 and 11:

Seid further discloses a plurality of customer premises equipment (CPE) edge routers each coupled to a respective one of said plurality of ingress routers (col. 5, 40-60)

Regarding claim 4:

Seid further discloses further comprising the access network (Figs. 1-3).

Regarding claims 5 and 12:

Seid further discloses a customer premises equipment (CPE) edge router to the access link (col. 5, lines 40-60).

Regarding claims 6, 13, and 18:

Seid further discloses said CPE edge router having a physical port coupled to said access link, said physical port implementing a first logical port for intra-VPN traffic and a second logical port for extra-VPN traffic (Figure 4).

Regarding claims 7, 14, and 19:

Seid further discloses at least one of said plurality of ingress routers implements a plurality of tunnels that logically partition intra- and extra-VPN traffic (col. 12, 20-30).

Regarding claims 8, 15, and 20:

Seid further discloses said one or more egress routers provide a plurality of different qualities of services to said intra-VPN traffic (col. 5, line 62 – col. 6, line 4).

Regarding claim 23:

Seid further discloses wherein the steps of receiving, determining, and forwarding the packet are performed at a customer premises router configured to process the packet (col. 5, lines 40-60; col. 8, lines 20-57). Although Seid does not explicitly mention the IP protocol or IP packets, Examiner takes Official Notice that it was well known in the art by the time the invention was made to transmit IP packets over the disclosed frame relay network hardware (see also Seid, col. 19. lines 48-57; for further reference consult the RFC 1490 reference from the Office Action of 7/24/06).

7. Claims 1-24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Applicant Admitted Prior Art (hereinafter, "AAPA") in view of Seid in view of Larson.

Regarding claims 1, 9, and 16:

AAPA discloses a method of providing a virtual private network (VPN) comprising one or more egress routers having connections to an access network including the access link, wherein said one or more routers transmit intra-VPN traffic and extra-VPN traffic to the destination host belonging to the VPN (page 3, line 13 – page 5, line 20; Figures 1 and 2), and a plurality of ingress routers coupled to the one or more egress routers for communication utilizing a network-based VPN protocol (Ibid).

AAPA does not disclose wherein intra-VPN and extra-VPN traffic are separated into a first and second logical connection, nor that the logical connections are partitioned such that denial of service attacks on said access link originating from sources outside the VPN are

prevented. However, Seid discloses a method for resisting denial of service attacks (i.e. network congestion, as taught by AAPA, page 5, lines 5-10) on any packet-switched network (col. 19, lines 48-57), comprising partitioning intra-VPN traffic and all extra-VPN traffic into a first and second logical connection (Figure 7, and col. 4, lines 1-10) in such a manner as to prevent denial of service attacks on said access link originating from sources outside the VPN (col. 2, line 56 – col. 3, line 15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to partition traffic between intra-VPN and extra-VPN sources as disclosed by Seid into the network disclosed by AAPA. The motivation for doing so would be to allow a network to provide and maintain a level of service to a VPN that is unperturbed by other traffic on the network, in a manner superior to that offered by the prior art (Seid: col. 2, lines 43-46; AAPA: page 5, lines 14-20).

Although Seid teaches in considerable detail how each VPN's logical connection should be guaranteed at least a minimum bandwidth regardless of the amount of traffic a node processes from sources other than said each VPN, Seid is silent regarding an explicit recitation of prioritizing VPN traffic over non-VPN traffic. However, this limitation would have been immediately obvious to one of ordinary skill in the art by the time of the invention, as evidenced by Larson teaching the same in a related invention (col. 43, lines 5-40). The claim is thus obvious not only because the ability to prioritize VPN traffic over non-VPN traffic for quality-of-service purposes was well within the normal abilities of one of ordinary skill of the art, but moreover the technique of prioritizing VPN traffic over non-VPN traffic actively prevents denial of service attacks on the VPN (Larson: col. 42, lines 40-60; col. 44, lines 1-15).

Regarding claims 2, 10, and 17:

AAPA and Seid disclose the limitations of Claims 1, 9 and 16 above. AAPA further discloses wherein the at least one of the plurality of ingress routers or the at least one or more egress routers logically partitions intra-VPN traffic and extra-VPN traffic using a differentiated services protocol to mark correspondingly the intra-VPN traffic and the extra-VPN traffic (AAPA: page 4, paragraph [09]).

Regarding claim 21:

AAPA discloses a known prior art method for providing a virtual private network (VPN), comprising assigning a first priority level to intra-VPN traffic flowing from sources included in the VPN (page 3, lines 1-11; page 4, line 14 – page 5, line 10); assigning a second priority level to extra-VPN traffic flowing from sources outside the VPN (Ibid), and transmitting intra-VPN and extra-VPN traffic from one or more egress boundary routers to the destination host (page 3, lines 13-22; Figure 1).

It is unclear from AAPA whether the traffic having the first priority level at the access link is granted precedence of access to the destination host belonging to the VPN over traffic having the second priority level, nor that the intra-VPN and extra-VPN traffic are transmitted over a first and second logical connections, respectively. However, Seid discloses the limitations regarding the priority levels (col. 10, lines 40-65; col. 12, lines 20-30) and the first and second logical connections (col. 2, line 56 – col. 3, line 15). It would have been obvious to one of ordinary skill in the art at the time the invention was made to partition intra-VPN and all extra-VPN traffic in the manner disclosed by Seid into the network disclosed by AAPA.

The motivation for doing so would be to better prevent denial of service attacks from affecting intra-VPN traffic (col. 3, lines 10-15).

Although Seid teaches in considerable detail how each VPN's logical connection should be guaranteed at least a minimum bandwidth regardless of the amount of traffic a node processes from sources other than said each VPN, Seid is silent regarding an explicit recitation of prioritizing VPN traffic over non-VPN traffic. However, this limitation would have been immediately obvious to one of ordinary skill in the art by the time of the invention, as evidenced by Larson teaching the same in a related invention (col. 43, lines 5-40). The claim is thus obvious not only because the ability to prioritize VPN traffic over non-VPN traffic for quality-of-service purposes was well within the normal abilities of one of ordinary skill of the art, but moreover the technique of prioritizing VPN traffic over non-VPN traffic actively prevents denial of service attacks on the VPN (Larson: col. 42, lines 40-60; col. 44, lines 1-15).

Regarding claim 22:

AAPA discloses a method of communicating, comprising receiving a packet that is destined to a host within a virtual private network (page 2, paragraph 04), and determining whether the packet is originated within the virtual private network or external to the virtual private network (page 3, paragraph 06).

AAPA does not disclose "forwarding the packet to the host over a first logical path or a second logical path based on the determination, wherein the first logical path is designated for traffic originating within the virtual private network and the second logical path is designated for traffic originating externally to the virtual private network". However, Seid

discloses these limitations (col. 2, line 49 – col. 3, line 14). It would have been obvious to one of ordinary skill in the art at the time the invention was made to partition intra-VPN and all extra-VPN traffic in the manner disclosed by Seid into the network disclosed by AAPA. The motivation for doing so would be to better prevent denial of service attacks from affecting intra-VPN traffic (col. 3, lines 10-15).

Although Seid teaches in considerable detail how each VPN's logical connection should be guaranteed at least a minimum bandwidth regardless of the amount of traffic a node processes from sources other than said each VPN, Seid is silent regarding an explicit recitation of prioritizing VPN traffic over non-VPN traffic. However, this limitation would have been immediately obvious to one of ordinary skill in the art by the time of the invention, as evidenced by Larson teaching the same in a related invention (col. 43, lines 5-40). The claim is thus obvious not only because the ability to prioritize VPN traffic over non-VPN traffic for quality-of-service purposes was well within the normal abilities of one of ordinary skill of the art, but moreover the technique of prioritizing VPN traffic over non-VPN traffic actively prevents denial of service attacks on the VPN (Larson: col. 42, lines 40-60; col. 44, lines 1-15).

Regarding claim 23:

AAPA further discloses wherein the packet is an Internet Protocol (IP) packet (page 3, paragraph 06), and the steps of receiving, determining, and forwarding are performed at a customer premises router configured to process the IP packet (Ibid; see also Seid, col. 5, lines 40-60).

Regarding claim 24:

AAPA [in view of Larson] further discloses wherein the packet over the first logical path is marked at a higher priority that the second logical path using a differentiated services protocol (page 4, paragraph 09).

Regarding claims 3-8, 11-15, and 18-20:

These claims are rejected for substantially similar reasons as discussed *supra* in the rejections of these claims in view of Seid and Larson.

Conclusion

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure, all of which illustrate the obviousness of the new limitation(s):

- U.S. Patent Publication 2002/0039352 to El-Fekih et al.
- U.S. Patent 7,215,637 to Ferguson et al.
- U.S. Patent 7,096,495 to Warrier et al.
- U.S. Patent 7,023,860 to Mauger et al.
- U.S. Patent 6,888,842 to Kirkby et al.
- U.S. Patent 6,765,921 to Stacey et al.
- U.S. Patent 6,680,922 to Jorgenson
- U.S. Patent 6,611,863 to Banginwar
- U.S. Patent 6,580,721 to Beshai

- "Quality of Service in IP Networks: Foundations for a Multi-service Internet" by Grenville Armitage further teaches that VPNs are inherently segregated into logical connections ["tunnels": pages 16, 17, and 181] while further suggesting the need for inventions like Seid, Larson, AAPA, etc. [pages 194-195, "A Look Ahead"], thus highlighting the general obviousness of the claimed invention

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 9:30am - 6:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

TAG
9/24/10
/Kimyen Vu/
Supervisory Patent Examiner, Art Unit 2435